View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Journal of King Saud University – Engineering Sciences (2016) xxx, xxx–xxx

King Saud University

Journal of King Saud University – Engineering Sciences

www.ksu.edu.sa
www.sciencedirect.com

SHORT COMMUNICATION

A secure data privacy preservation for on-demand cloud service

Chandramohan Dhasarathan *, **Vengattaraman Thirumal, Dhavachelvan Ponnurangam**

Department of Computer Science, School of Engineering & Technology, Pondicherry University, Pondicherry, India

Received 10 October 2013; accepted 20 December 2015

KEYWORDS

Privacy;
Cloud storage;
Identity access management;
Digital Data Loss

Abstract This paper spotlights privacy and its obfuscation issues of intellectual, confidential information owned by insurance and finance sectors. Privacy risk in business era if authoritarians misuse secret information. Software interruptions in steeling digital data in the name of third party services. Liability in digital secrecy for the business continuity isolation, mishandling causing privacy breaching the vicinity and its preventive phenomenon is scrupulous in the cloud, where a huge amount of data is stored and maintained enormously. In this developing IT-world toward cloud, users privacy protection is becoming a big question , albeit cloud computing made changes in the computing field by increasing its effectiveness, efficiency and optimization of the service environment etc, cloud users data and their identity, reliability, maintainability and privacy may vary for different CPs (cloud providers). CP ensures that the user's proprietary information is maintained more secretly with current technologies. More remarkable occurrence is even the cloud provider does not have suggestions regarding the information and the digital data stored and maintained globally anywhere in the cloud. The proposed system is one of the obligatory research issues in cloud computing. We came forward by proposing the Privacy Preserving Model to Prevent Digital Data Loss in the Cloud (PPM–DDLC). This proposal helps the CR (cloud requester/users) to trust their proprietary information and data stored in the cloud.

© 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

Cloud computing is one of the massive and major research areas in both the industrial and academic fields and many researchers have been working toward its research issues. As the cloud came into existence a lot of issues also surrounded it. Normally cloud computing has mostly common and general issues like interoperability, SLA-(service level agreement), universal standards, unique approach for all cloud providers, data

* Corresponding author.
E-mail addresses: pdchandramohan@gmail.com (D. Chandramohan), vengattaraman.t@gmail.com (T. Vengattaraman), dhavachelvan@gmail.com (P. Dhavachelvan).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksues.2015.12.002
1018-3639 © 2015 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Please cite this article in press as: Chandramohan, D. et al., A secure data privacy preservation for on-demand cloud service. Journal of King Saud University – Engineering Sciences (2016), http://dx.doi.org/10.1016/j.jksues.2015.12.002

portability among different clouds, various security issues and mainly privacy protection to users secret and confidential information. The cloud elucidation is interoperable and companionship with homogeneous services to benefits all sorts of business needs at earliest without effecting the privacy. CP consists of different layers for information dealing and on-demand provisioning of computational resources.

Data stored in the cloud are accessible to users in the form of different services with the help of traditional networks and it is also known to be the cloud storage, in which it holds a brief description about cloud user profiles, business details and back up information to make available ubiquitously via internet as backbone. Online data backup, data archiving, data compliances, disaster recovery, and compliance regulations are some of the issues in cloud data storage. Many technologies have been developed for cloud data storage and portability of information transfer among different cloud providers and it is mainly based on the cloud provider's service level agreements and policy. In this fast developing cloud business world users are permitted to exchange their data stored from one provider to other as a portability option.

In this context the providers should ensure the privacy protection strategies or enrich the issues pertained along with their storage and recovery. Leading cloud providing companies are farm-outing their customers information to cloud back up service providers as an infrastructure and power maintenance policy. To reduce the doubt or increase trust among user's about their information management, some nominal metrics should be adopted to identify the maximum possibility of storing information. There may be many risk factors evaluated along with this as a data offsite replication and data disaster recovery as a privacy issue for both providers and consumers. At administration level the need for cloud storage as been adopted in several principles to serve their clients on demand at all circumstances with high privacy and security.

2. Background and related work

To avoid unlawful information disclosures Breaux and Anton, 2008, derived a method to support the software engineering effort to derive security requirements from regulations; in which the methodology for directly extracting access rights and obligations from regulation texts. The methodology provides statement-level coverage for an entire regulatory document to consistently identify and infer six types of data access constraints and assign required priorities between access rights and obligations. Liu and Chen (2011), designed a VGuard framework with an efficient protocol that allows a cloud policy owner and a cloud request owner to collaboratively determine whether the request satisfies the policy without the policy owner knowing the request and the request owner knowing the policy. Xiong et al. (2011), proposes a cost-aware resource management system based on SLA-service level agreement termed as SmartSLA which consists of two main components: the system modeling module and the resource allocation decision module. To prevent the online social community Li et al. (2011), shows his interest in group based privacy-preserving recommender system called Pistis. The identification of inherent item-user's interest group and separating them with private interests and public interest might improve the solidity, and help to fasten and accurately transmit emergency data Liang et al. (2011), through an emergency call scheme by enabling patients in life-threatening emergencies to call the nearby helpers via mobile healthcare social networks. To facilitate interoperations among the applied cryptographic mechanisms Lee et al. (2011), applied the policy regulation with the HIPAA (Health Insurance Portability and Accountability Act), for a flexible cryptographic key management solution. Chandramohan et al. (2014, 2015a,b), proposed a testbed for evaluating the efficiency of services by filtering its functional and non functional QOS-(Quality of Services) parameters. Web service personalization and suitability in cloud as mathematical evaluation the QOS parameters are verified for different service efficiency.

Kadloor et al. (2012), proposal to develop a dynamic program to compute the optimal privacy preserving policy that minimizes the correlation between user's traffic and adversary's waiting times of the cloud user. Hong et al. (2012), propose a new MapCG model as a map-reducing framework to provide source code level portability between CPUs (central processing units) and GPUs (graphics processing units). Chang and Choi (2010), cloud computing is the upcoming trend in the IT business world and faces a lot of challenges in technical matters and security issues. In his proposal the author described the crucial needs of cloud computing technological features, and challenges and also cloud computing security. Hussin et al. (2012), proposed a new era of using privacy manager in the cloud to control all features of cloud providers and to control all their policy based obfuscation and de-obfuscation. To enhance the usability of this approach the author proposed his own approach to evaluate the performance and its scalability. Chandramohan et al. (2012), provided a protocol for authentication purpose with an user identity based key management system to minimize the data lose.

Pieters (2011), describes the major research issues in recent development in the cloud and its security issues, the ethical implication and privacy issues can be viewed and monitored using his proposed bird's eye view approach. In his approach he covered the disappearing boundary of the cloud and encryption standards in use, its physical security properties etc. Ruiter and Warnier (2011), in his approach describes the privacy regulations for cloud leads to the occurrence of uncertainty. Troncoso-Pastoriza and Perez-Gonzalez (2010), expresses the landscape signal processing cryptographic technique to maintain the private information of cloud users and clients of cloud providers. The author briefly explains the fundamental background of the cloud and its issues from the day it originates. Vaquero et al. (2011), describes many issues and problems getting increased daily in the cloud and the author proposed a few access controls and encryption techniques to solve the privacy issues in cloud computing virtualized data centers. Grodzinsky and Tavani (2011), adopts the Helen Nissenbaum's theory as a framework of privacy as contextual integrity for evaluating the cloud providers services, which depends on decision heuristic model. Murugaiyan et al. (2014), describes the preventing mechanism for cloud user and their data could be organized using a framework approach. While addressing the cloud concepts over the past several years there presents many cloud computing service models and the risk migration in it. The main goal to standardize the service level agreements and policies adapted for maintaining privacy and enhancing the security in cloud describes

Please cite this article in press as: Chandramohan, D. et al., A secure data privacy preservation for on-demand cloud service. Journal of King Saud University – Engineering Sciences (2016), http://dx.doi.org/10.1016/j.jksues.2015.12.002

the privacy prevention line of attack in an assortment of user adoptable scenario.

3. Proposed system

This approach focuses on the portability issue in the cloud, users can hold their account details and information along with respective trusted cloud providers, it get pursued until the user marks their position as uncomfortable with a particular CP. Even cloud provider's suggestion may be unsuccessful during back tracking the client information maintained by them. They do not have a clear identification as to where the actual data resides inside their CP cloud. By using this proposal our main objective is to resolve this issue at a minimum risk and maximum benefit to both the providers and users. Habitually data have the public attributes to map the evasion and measure of uncertainty to be a private information. The information about the hidden data would reflects its revealed data presented in the cloud. Thereby, public and private cloud providers should protect data in various vicinity such as categorical data, optimal input, eliminated low probabilities, equivalent aggregation, Gaussian distribution, side information and successive disclosure are monitored to be reliable and secure in the cloud.

Noisy interruption in the prescribed data source of cloud providers, instigate a scheme to avoid privacy leakage. Petri net based models emerged as a modeling tool for proposing our own system which demonstrates concurrency, synchronization and uncertainty. The use of stochastic Petri nets has become particularly important in the modeling of automated modeling for the cloud system. The Petri-net process is encouraged to develop distributed theories and techniques. It can be used to analyze both logical and quantitative processes. In Fig. 1 security is one of the most important frames for a cloud provider as it will utilize data storage and transmission encryption, user authentication, and authorization, all a cloud user's concern about the liability of isolated data accessed by criminals like hackers, intruders, and annoyed employees. Cloud

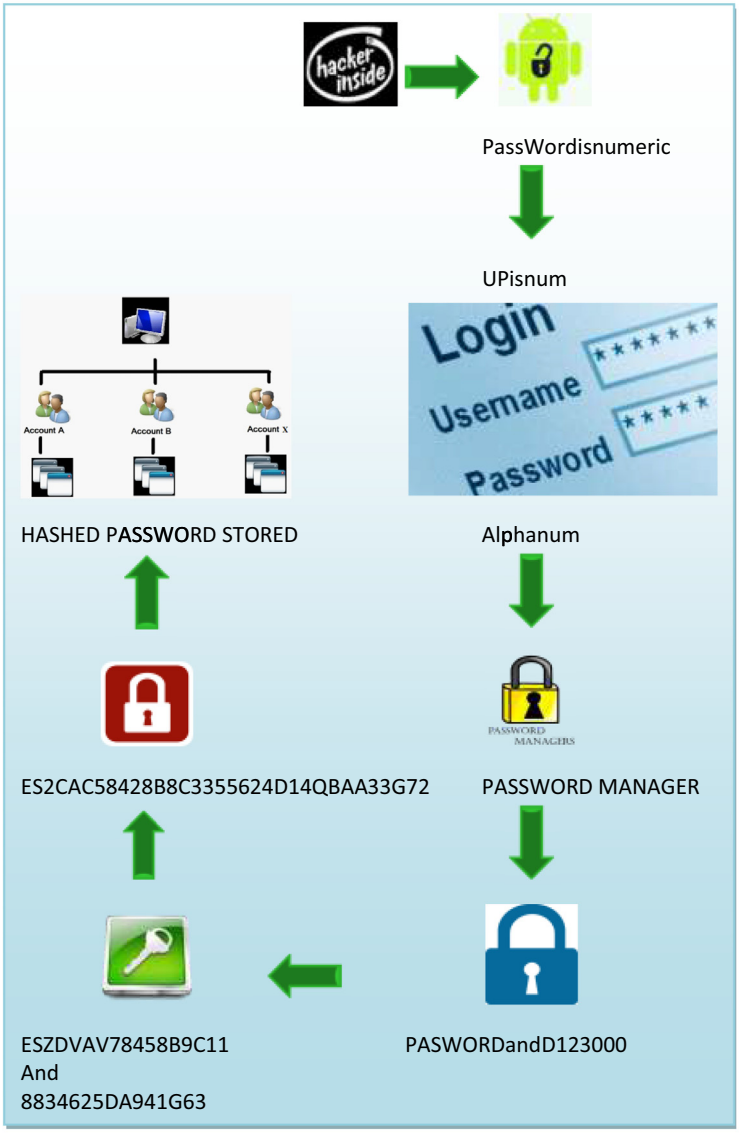

Figure 1 PPM–DDLC anomaly detection process.

providers are extremely aware of this problem and applied extensive possessions to extenuating this kind of distress. Reliability and trustworthiness are also the main issues to feel uncomfortable with for cloud providers both financially and technologically in the current market. By using superfluous storage techniques some CPs modify the original data stored within them and lead to signing off from one provider to another. Ownership of CR data has been transferred to the cloud; some users are concerned that they could lose several data or CP thinks all their rights are incapable of protecting the rights of their beloved customers.

3.1. PPM–DDLC algorithm

Step 1: Start.
Step 2: Select the features from the list of anomalous examples.
Step 3: Choose the best fit anomaly x_i that might be indicative of a defined system.
Step 4: Fit parameters are $\mu_1, \ldots \mu_n, \sigma_1^2, \ldots \sigma_n^2$.
Step 5: For $\mu_n \leqslant$ fit parameter repeat until null
Step 6: $\mu_j = \frac{1}{m}\sum_{i=1}^{m} x_j^{(i)}$ Verify and validate
Step 7: $\sigma_3^2 = \frac{1}{m}\sum_{i=1}^{m}(x_j^{(i)} - \mu_j)2$
Step 8: Compute $(x, p(x))$.
Step 9: $p(x) = \prod_{j=1}^{n} \pm p(x_j; \mu_j, \sigma_3^2)$
Step 10: Repeat until $\mu_n \neq \phi$; $\prod_{j=1}^{n} \frac{1}{\sqrt{2\pi}\sigma_3} \exp\left\{-\frac{(x_j-\mu_j)^2}{2\sigma_3^2}\right\}$
Step 11: Anomaly if $p(x) < p(x) < \delta$; End;

Data portability policy

A cloud provider came across issues of data portability in such a way that users have a request for it. We are initiating a model which may help to frame an open standard because we believe in advancing this open effort. However the CP should not be permitted to change its policy on a demand of its own. Very few cloud provider companies have already launched portability policies. The portability policy proposal is still in its preschool stages and will nurture as awareness increases, with more unambiguous questions emerging when issues are recognized. CP and SN (social network) providers will need to pay finicky consideration to the projected right for users to port their personal information to another CP, as well as their right to erase their information. PPM–DDLC algorithm for CR to port their data to a new CP will also be an explicit anxiety to SN whose servers continue to edge over with user information. The right for CR to involve along with CP to relocate their data to a new CP should promote cloud shopping. This

Table 1 Privacy during data interoperability.

Service provider	Google	Microsoft	Amazon	IBM
CP1	0	9.37	2.95	2.85
	3.49	0.95	3.74	0.79
	6.38	1.35	2.76	1.13
	9.47	6.38	0.39	1.81
	1.76	0.64	3.71	0.04
CP2	5.45	4.95	2.64	3.19
	1.14	1.15	0.67	8.84
	2.43	1.39	9.74	4.67
	2.42	3.51	4.3	4.7
	2.41	3.92	1.98	4.09
CP3	0.21	1.04	0.21	0.11
	0.13	0.9	0.21	0.71
	0.16	0.91	0.31	0.08
	0.91	1.05	0.12	0.72
	0.52	0.1	0.17	0.5
CP4	0.95	0.19	1.7	0.17
	1.57	0.24	0.2	0.9
	1.8	0.3	0.51	0.21
	0.75	0.2	0.81	0.13
	0.59	0.3	0.71	0.27
	1.2	1.2	0.61	0.3
CP5	0.13	0.5	0.5	0. 1
	0.68	1.6	0.01	0.9
	1.09	0.8	0.1	0.1
	0.12	0.4	1.2	0.37

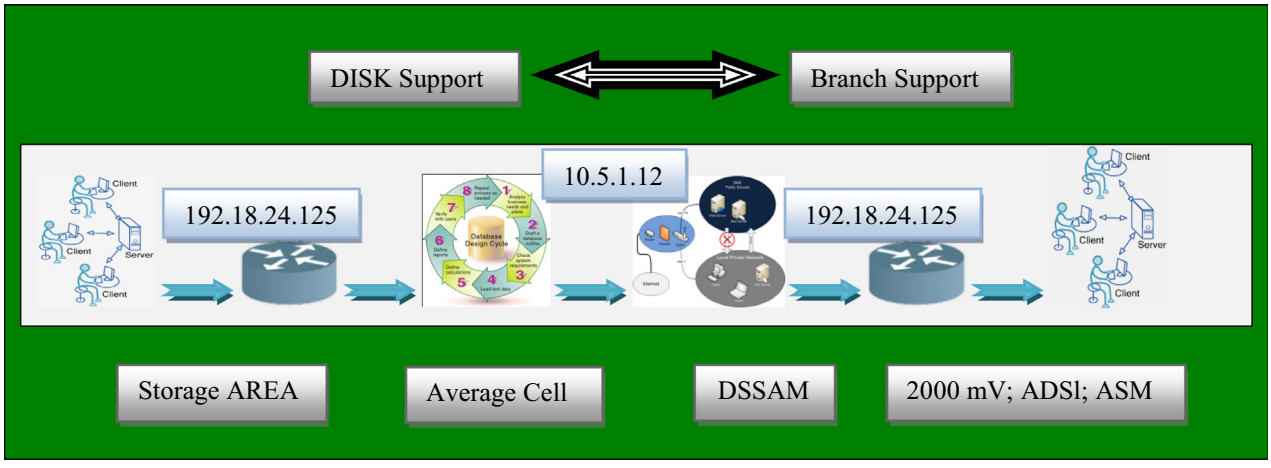

Figure 2 PPM–DDLC model.

Table 2 Cloud data privacy evaluation in typical mode.

CP1	CP2	CP3	CP4	CP5	CP6	CP7
1.7	0.55	0.26	0.03	3.54	0.63	0.77
1.1	1.28	0.39	0.3	4.07	0.77	0.46
1.6	0.75	0.35	0.21	3.91	0.5	0.65
1.9	2.23	0.44	0.01	5.58	1.15	0.69
0.02	0.94	0.56	0.5	3.02	0.55	0.9
1.05	5.1	0.52	0.16	7.83	1.75	0.35
2.18	1.27	0.67	0.7	5.82	1.05	0.09
0.91	1.05	0.12	0.72	3.8	0.7	0.4
0.52	0.1	0.17	0.5	2.29	0.25	1.05
7.1	0.95	0.76	0.08	9.89	2.22	0.8
3.14	0.46	0.89	0.91	6.4	1.3	0.04
1.09	0.60	1.04	0.10	3.83	0.77	0.75
2.05	1.05	1.17	0.1	5.37	1.05	0.35
1.13	1.60	1.34	0.18	5.25	1.5	0.31
0.1	0.9	0.21	0.71	2.92	0.4	0.9
0.6	0.91	0.1	0.08	2.69	0.2	0.95
0.9	1.05	0.1	0.72	3.77	0.65	0.75
1.56	0.76	0.4	0.4	4.12	0.8	0.64
0.2	1.15	1.4	0.78	4.53	0.85	0.55
0.78	2.34	1.7	0.65	6.47	1.37	0.04

will encourage larger antagonism between cloud providers. One of the most valuable weapons for CRs to have in their hand is to switch different providers. This is an idyllic policy that should be pursued by all CP.

Many researchers have been repeatedly initiating the framing of a universal standard format which helps a provider to permit other business competitive providers to gasp different CP technologies, and it should be compatible to new CP technologies which make an effortless transformation, which is achievable to normalize the user's personal information and data Fig. 2. These migration possibilities should be informed to all CR and users as a different cost for transporting their data.

Cloud providers have their own flexibility while framing their privacy laws which may vary between companies; it is even directly proportional to the national law and order schemes and it also differs as per the country's violations. It's mainly due to the initiation of information leverage of customers who are involved in some illegal activities against a nation's internal security and maintain's their military secrets and other secrets about bordering nations and so on.

4. Experimental result analysis and evaluation

We evaluated cloud users data privacy in our cloud environment with different global cloud provider's names as follows in Tables 1 and 2. Similarly their impacts are plotted and their variations explained with a graph Figs. 3 and 4.

In cloud portability unauthorized users entry gets breached and privacy starts as the elapsed time is 1.4 s. In cloud interoperability unauthorized users entry gets breached and privacy starts if the elapsed time is 1.2 s. If a cloud user is willing to switchover from one provider to another first the provider should ensure all his historical references and e-discovery backups are completely removed from the source and gets

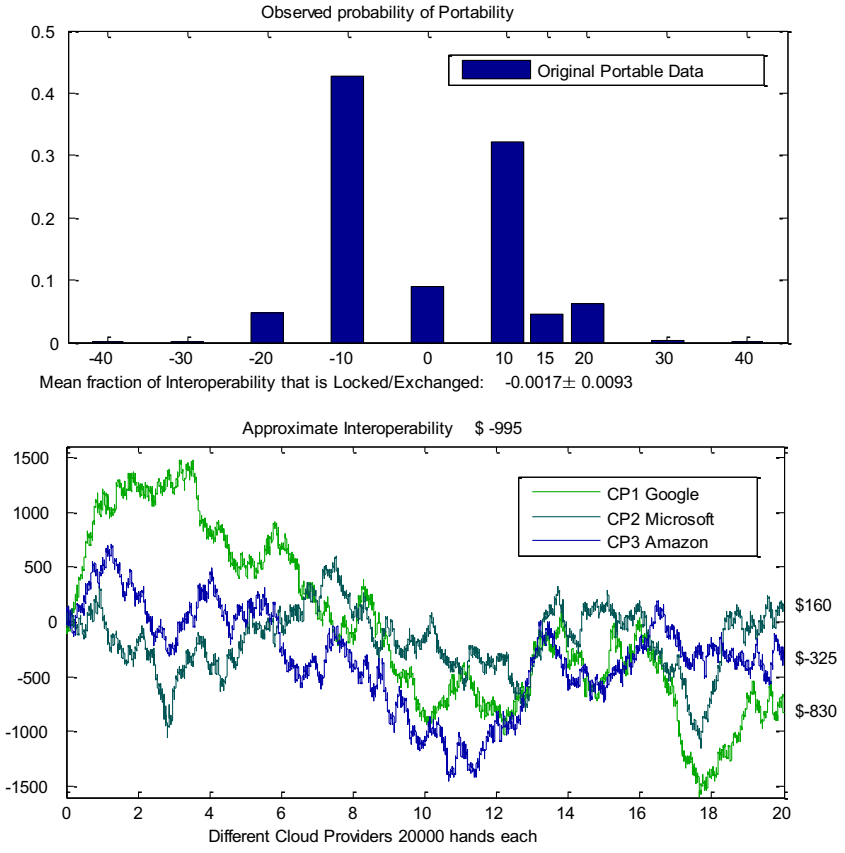

Figure 3 Data privacy protection in inter-cloud cost effectiveness.

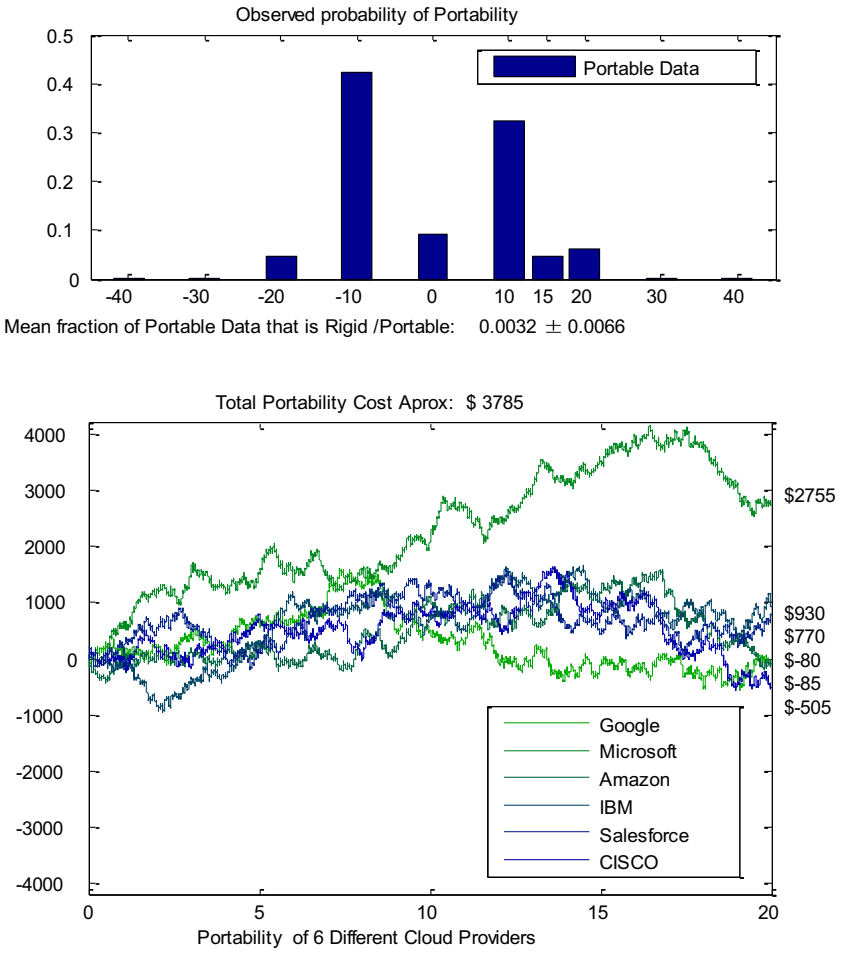

Figure 4 Cloud data portability cost effectivness.

inserted or stored in another cloud provider in whom the clients want to have his data or information, here cloud archiving and aggregation plays an important role to give surety to both providers and users.

The archiving will chose the best provider based on their back up storage and its mining information. During integration the main and real portability issue will be the hitting peak for all CP-cloud providers. Some CPs chose limited service level agreements as a safety measure to hold their clients with them. All these portability issues are combined together and make a question mark for future cloud storage and cloud computing itself. Still it's a research issue and one cannot enjoy full-fledged cloud computing benefits until a strong SLA agreement or global standard is framed to resolve these issues. We are proposing a hybrid authentication technique as a proposal as a milestone in solving the portability issue. In this paper an end point lock approach is designed by detecting the anomaly operations and providing hash authentication coupled with the Diff–Hallman exchange protocol, all these approaches combined together as a hybrid model to solve the portability issue in the cloud with the Privacy Preserving Model to Prevent Digital Data Loss in the Cloud (PPM–DDLC). Our proposed representation of the PN (Petri-Net) model acts as superfluous impedance for cloud providers to check different module looms to conclude with legitimate properties of the habitual Petri-net. Hierarchical intelligent Privacy Preserving Model is designed as per evaluation criteria of all possible parameters going on to process the user's request and response, and will depend on the same evaluation with cent-percent guaranty to preserve users data.

5. Conclusion

In this paper we studied and analyzed various techniques and explored them as survival of the fittest in the cloud environment. Proposed approach get fulfilled only when both cloud providers and cloud requestors/end-users ensure all their data have their own privacy policy even if they agreed to choose different cloud providers to store or exchange data as per portability and interoperability of privacy law and pertain its issues, researchers can hope this proposal will prove to be a useful foundation for solving their issues on privacy for cloud in all stipulated areas. In future we are taking forward this research to implement in each and every layer of CA and to enhance the model with an advanced policy and come up with a tool having its own framework which can be interoperable with all cloud providers and all advanced latest technologies yet to emerge in the IT industry. It will develop more trust and a new standard in cloud architecture and become a new era of the next level of research in clouds. The proposed approach helps the cloud providers to have a universal standard privacy policy for CA. Moreover, this paper examines the privacy awareness

Please cite this article in press as: Chandramohan, D. et al., A secure data privacy preservation for on-demand cloud service. Journal of King Saud University – Engineering Sciences (2016), http://dx.doi.org/10.1016/j.jksues.2015.12.002

and importance of the user's secrecy being preserved in the current ubiquitous mobile cloud computing world. Data stored in the cloud have highly sensitive information. Once private information gets misused, the probability of privacy breaching increases which thereby reduces the user's trust on cloud providers. In the modern internet world, information management and maintenance are one among the most decisive tasks. Information stored in the cloud by the finance, healthcare, government sectors makes it all the more challenging since such tasks are to be handled globally.

References

Breaux, Travis D., Anton, Annie I., 2008. Analyzing regulatory rules for privacy and security requirements. IEEE Trans. Software Eng. 34 (1), 5–20.

Chandramohan, D., Vengattaraman, T., Basha, M.S.S., Dhavachelvan, P., 2012. MSRCC–mitigation of security risks in cloud computing. In: Springer Book Series-AISC-2012, vol. 176, pp.525–532. http://dx.doi.org/10.1007/978-3-642-31513-8_54.

Chandramohan, D., Vengattaraman, T., Dhavachelvan, P., 2014. Data privacy breach prevention framework for the cloud service. Secur. Commun. Networks, 1939-0122 8 (6), 982–1005. http://dx.doi.org/10.1002/sec.1054.

Chandramohan, Dhasarathan, Sathian, Dananjayan, Rajaguru, Dayalan, Vengattaraman, Thirumal, Dhavachelvan, Ponnurangam, 2015a. A multi-agent approach: to preserve user information privacy for a pervasive and ubiquitous environment. Egypt. Inf. J., 1110-8665 16 (1), 151–166. http://dx.doi.org/10.1016/j.eij.2015.02.002.

Chandramohan, Dhasarathan, Rajaguru, Dayalan, Vengattaraman, Thirumal, Dhavachelvan, Ponnurangam, 2015b. A new privacy preserving technique for cloud service user endorsement using multi-agents. Elsevier J. King Saud Univ. – Comput. Inf. Sci., 1319-1578. http://dx.doi.org/10.1016/j.jksuci.2014.06.018.

Chang, Hyokyung, Choi, Euiin, 2010. Challenges and Security in Cloud Computing. Springer, pp. 214–217.

Grodzinsky, F.S., Tavani, H.T., 2011. Privacy in "the cloud": applying Nissenbaum's theory of contextual integrity. ACM SIGCAS Comput. Soc. Arch. 41 (1), 266–270.

Hong, Chun-Tao, Chen, De-Hao, Chen, Yu-Bei, Chen, Wen-Guang, Zheng, Wei-Min, 2012. Providing source code level portability between CPU and GPU with MapCG. Springer J. Comput. Sci. Technol. 27 (1), 42–56.

Hussin, Mohamad Fahmi, Wang, Bin, Hipnie, Ramani, 2012. The reliability and validity of basic offshore safety and emergency training knowledge test. J. King Saud Univ. Eng. Sci., 1018-3639 24 (2), 95–105. http://dx.doi.org/10.1016/j.jksues.2011.05.002.

Kadloor, Sachin, Gong, Xun, Kiyavash, Negar, Venkitasubramaniam, Parv, 2012. Designing router scheduling policies: a privacy perspective. IEEE Trans. Signal Process. 60 (4), 2001–2012.

Lee, Chien-Ding, Ho, Kevin I.-J., Lee, Wei-Bin, 2011. A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations. IEEE Trans. Inf. Technol. Biomed. 15 (4), 550–556.

Li, Dongsheng, Lv, Qin, Xia, Huanhuan, Shang, Li, Lu, Tun, Gu, Ning, 2011. Pistis: a privacy-preserving content recommender system for online social communities. In: IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, pp. 79–86.

Liang, Xiaohui, Lu, Rongxing, Chen, Le, Lin, Xiaodong, Shen, Xuemin (Sherman), 2011. PEC: a privacy-preserving emergency call scheme for mobile healthcare social networks. IEEE J. Commun. Networks 13 (2), 102–112.

Liu, Alex X., Chen, Fei, 2011. Privacy preserving collaborative enforcement of firewall policies in virtual private networks. IEEE Trans. Parallel Distrib. Syst. 22 (5), 887–895.

Murugaiyan, S.R., Chandramohan, D., Vengattaraman, T., Dhavachelvan, P., 2014. A generic privacy breach preventing methodology for cloud service. Int. J. Grid High Perform. Comput., 1938-0259 6 (3), 56–88. http://dx.doi.org/10.4018/ijghpc.2014070104.

Pieters, Wolter, 2011. Security and privacy in the clouds: a bird's eye view. Computers, Privacy and Data Protection: An Element of Choice. Springer, pp. 445–457.

Ruiter, Joep, Warnier, Martijn, 2011. Privacy regulations for cloud computing: compliance and implementation in theory and practice. Computers, Privacy and Data Protection: An Element of Choice. Springer, pp. 361–376.

Troncoso-Pastoriza, Juan Ramon, Perez-Gonzalez, Fernando, 2010. CryptoDSPs for cloud privacy. In: WISE 2010 Workshop, LNCS 6724. Springer, pp. 428–439.

Vaquero, Luis M., Rodero-Merino, Luis, Morán, Daniel, 2011. Locking the sky: a survey on IaaS cloud security. Comput. Springer, 93–118.

Pengcheng, Xiong, Yun, Chi, Shenghuo, Zhu, Hyun Jin, Moon, Calton, Pu, Hakan, Hacigumus, 2011. Intelligent management of virtualized resources for database systems in cloud environment. In: IEEE ICDE Conference, pp 87–98.